犯罪の未然防止・再犯防止と情報の取扱いに関する覚書き

星　周一郎

はじめに

近年、犯罪の未然防止、再犯防止への要求は、ますます高まりを見せている。また、犯罪が発生した際のより的確な初動対応への要請も、被害者の保護という観点も含めてであるが、より高いレベルのものが求められている。もちろん、これらの要求について、警察をはじめとする法執行機関や行政機関、関係 NPO 法人などが連携して対応をする体制が、従来からも整えられており、犯罪被害の防止に一定の成果を上げていることも、改めて述べるまでもない。

これらの対応を考えるにあたって重要なのが、情報の取り扱いである。犯罪の未然防止のためには、犯罪機会を減少させるための全般的な取り組みも重要

であるが[1]、より個別的には、「不審者」についての情報を正確に把握し、適正に用いることで、的確な対応をすることが求められることにもなる。

そこで、本稿では、アドホックな形でしかないが、いくつかの場面を取り上げ、それぞれの場面ごとの検討を通じて、犯罪防止という文脈で用いられる情報の取扱いに関して簡単な考察を加えることにしたい。

1　サイバーセキュリティにおける情報共有

(1) サイバーセキュリティのための情報共有の必要性

インターネットに代表されるICT技術の進展により、IoTを初めとして、社会がますますその依存度を高めていることは、改めて述べるまでもない。それに伴い、「サイバー犯罪」も多様化の様相を示しており、そこでは「犯罪の縮図」が体現されつつあるといってもよい。そして一方では、属人性の高いインターネット接続端末、とりわけスマートフォン機器などを利用した業務妨害事案、名誉毀損事案、児童ポルノ・児童買春防止法違反事案などは、アクセスログが保存されている限り、現実世界における犯罪よりも、被疑者を容易に特定することができる。他方で、標的型攻撃メール、ボットネットへの感染、サイバーテロなど、洗練された手段を用いた犯罪の登場は、サイバー空間の脅威として、不断の対策を要する課題を生じさせている。

後者の問題の深刻さ、およびより効果的な対応の必要性は、以前から認識されてきたところである。アメリカでは、サイバー空間の脅威に対処するための産学官の情報共有と協力を促進すべく、産業界、学術機関および法執行機関が保有するサイバー空間の脅威に関する情報を業界横断的かつリアルタイムに収集・分析し、サイバー空間の脅威に共同で対処するための枠組みとして、

1)　たとえば、田中法昌「我が国の犯罪予防対策の概況」警察政策研究13号（2009年）65頁、山本俊哉「日本における環境設計を通した犯罪予防（CPTED）の適用と展開」刑法雑誌54巻3号（2015年）426頁以下。

NCFTA（National Cyber-Forensics & Training Alliance）が 1997 年に設立された。そして、創設以来、上記産学官が一体となって先制的・包括的な対応を行うことで、サイバー空間における金融サービスを悪用した犯罪の捜査に関連した多額の犯罪収益の押収や被害の未然防止に貢献するなど、サイバー空間の脅威に起因する被害の予防、拡大防止、検挙等に多大な成果をあげており[2)]、同様の試みがアメリカ以外にも拡がりつつある[3)]。

このような事情は、わが国においても例外ではない。わが国においても、以前からインターネット・サービス・プロバイダーなどが中心となって、サイバー攻撃等の情報収集・分析および対応について情報共有の仕組みとして、「Telecom-ISAC Japan」が、また平成 28 年 3 月からはそれを発展的に継承した「ICT-ISAC」が発足し、また、金融機関によるサイバーセキュリティに関する情報の共有・分析を行う「金融 ISAC」が発足している。さらに、インシデントに対する早期対応を図るべための CSIRT（Computer Security Incident Response Team）の取り組みにおいて、JPCert コーディネーションセンターが、インターネット等を介して発生するインシデント情報やセキュリティに対する脅威について、業種横断的に、報告を受け、対応の支援や再発防止のための対策の検討と助言を行うほか、それらを介した発生状況、手口の分析などを踏まえた脅威の回避策を発信し、情報共有を促進している。

しかし、より効果的なサイバーセキュリティの枠組みは、サイバーセキュリティへの脅威を生じさせている者を確定し、それを検挙することに求められるであろう。先に言及したアメリカの NCFTA は、産業界、学術機関に加えて、法執行機関が関与して、それぞれが保有するサイバー空間の脅威に関する情報

2)　警察庁総合セキュリティ対策会議『サイバー空間の脅威に対処するための新たな産学官連携の在り方～日本版 NCFTA の創設に向けて～（平成 25 年度総合セキュリティ対策会議報告書)』（2014 年）1 頁以下。

3)　カナダにおける組織として、NCFTA Canada（National Cyber-Forensics and Training Alliance Canada)、イギリスの組織として CDA（Cyber Defence Alliance）などがある。

を共有するという点で、このような、より効果的なサイバーセキュリティ対策に資する枠組みであると考えられる。わが国においても、平成 25 年に、日本版 NCFTA として「日本サイバー犯罪対策センター（Japan Cybercrime Control Center・JC3)」が設立され、すでに一定の成果を上げているところである[4)]。

なお、これらのサイバーセキュリティ対策にとって必要な情報というのは、基本的にインシデントに関するものに限られることが多いと考えられ、そうである限り、その情報は、いわゆる個人情報にはあたらないことになる。それゆえ、そういった情報の取扱いに関しては、たとえば、個人情報保護法上の規制対象にはなりえない。

(2) 捜査情報の犯罪防止のための利用

だが、すでに見たように、これらのサイバーセキュリティ情報について、民間企業や民間組織において分析することには限界がある。

---

4)　拙稿「サイバーセキュリティへの刑事法的対応に関する一考察」法学会雑誌 56 巻 1 号（2015 年）371 頁、警察庁総合セキュリティ対策会議『サイバー犯罪捜査及び被害防止対策における官民連携の更なる推進（平成 27 年度総合セキュリティ対策会議報告書)』(2016 年）1 頁参照。さらに、警察では、不正プログラム対策協議会（ウィルス対策ソフト提供事業者等との間で、新たな不正プログラム等の情報を提供するなどして、ウィルス対策ソフトの更新等により、IT ユーザー全体のセキュリティ対策を向上する枠組み)、不正通信防止協議会（セキュリティ関連事業者との間で、不正プログラム等による通信の接続先等の情報を共有することで、わが国事業者等による不正な接続先への通信を防止する枠組み)、サイバーインテリジェンス情報共有ネットワーク（情報窃取の標的となるおそれのある先端技術を有する事業者等と、情報窃取を企図したとみられるサイバー攻撃に関する情報を共有する枠組み)、サイバーテロ対策協議会（各都道府県に設置したもので、管内の重要インフラ事業者等との間で、サイバー攻撃に関する情報を共有する枠組み)、共同対処協定の締結（オンラインゲーム事業者や銀行等との間で、信頼関係を構築し、警察への通報を促進する等することで、サイバー犯罪の潜在化の防止や捜査活動の効率化・再発防止を図る枠組み）などの形で、官民連携の推進が図られている。警察庁編『平成 28 年版警察白書』(2016 年）132 頁。

これに対して、これらサイバーセキュリティに関するインシデントが、何らかの犯罪を構成するのであれば、警察による捜査権限を行使した捜査がなされることになる。この場合、「事案の真相を明らかに」することを目的として、刑事訴訟法に定められた強制処分の行使も含めた証拠収集がなされることになるが、それはあくまでも、「刑罰法令を適正且つ迅速に適用実現することを目的とする」（刑事訴訟法 1 条）ものである。ところが、洗練されたサイバー攻撃は、得てして国外から行われていることもあり、現実問題として犯人の検挙に至らない場合も多い。そういった場合には、当該捜査に基づいて収集された証拠から得られる情報は、事件が起訴されるわけでもないから、そのまま捜査機関のもとに「お蔵入り」することになってしまう。

だが、そこで得られた情報は、同時に、サイバーセキュリティ、すなわちサイバー攻撃やサイバー犯罪を防止するための有益な情報であることも多い。そして、「犯罪防止」の観点からすれば、このような情報の活用をも図ることで、個別事案限りのアドホックな対応ではなく、より大局的、戦略的な観点からの被害防止対策が可能となる。こういった施策が、今後ますます必要となることが予想されるとするならば、これら捜査で得られた情報のうち、被害防止に有効なものについては、それを積極的に活用していくことが考えられる。

その可能性を考えるにあたっては、公判開廷前段階において、訴訟に関する書類を公にすることを原則として禁止する刑事訴訟法 47 条との関係をどのように整理すべきかが問題となる。これは、「訴訟に関する書類が公判開廷前に公開されることによって、訴訟関係人の名誉を毀損し公序良俗を害しまたは裁判に対する不当な影響を引き起すことを防止する趣旨」の規定であると解されている[5)]。そして、同条但書は、公益上の必要その他の事由があって、相当と認められる場合には、公判開廷前の書類を公にすることを認めている。この「相当と認められる」か否かの判断に当たっては、前記 47 条および同条但書の趣旨を踏まえると、「『訴訟に関する書類』を公にすることを相当と認めるこ

5)　最判昭和 28 年 7 月 18 日（刑集 7 巻 7 号 1547 頁）。

とができるか否かの判断は，当該「訴訟に関する書類」を公にする目的，必要性の有無，程度，公にすることによる被告人，被疑者及び関係者の名誉，プライバシーの侵害等の〔前記の〕弊害発生のおそれの有無等諸般の事情を総合的に考慮してされるべきものであり，当該『訴訟に関する書類』を保管する者の合理的な裁量にゆだねられている」とされている[6]。より具体的には、公にする利益（目的、必要性）とこれによって予想される弊害とを利益衡量し、合理的な裁量で決すべきことになる[7]。

それを踏まえると、ますます深刻さの度合いを深めるサイバーセキュリティに対する脅威への対応の必要性という「公にする利益」と、それを公にすることによって予想される弊害とを比較衡量した上で、たとえばであるが、①セキュリティベンダーなどのより専門的な技術者にとって必要な情報であるか、②より広くセキュリティ担当者にとっても必要な情報であるか、③一般の利用者にとっても周知が必要であって世間一般に公にすることが望ましく、またそれに伴い予想される弊害も大きくない情報であるかなど、対象情報の性質をも加味しつつ、これらの情報を適切な形態・範囲で共有、公表するなどして、積極的に利用していくことが考えられる。

---

6)　最決平成 16 年 5 月 25 日（民集 58 巻 5 号 1135 頁）。

7)　河上和雄ほか編『注釈刑事訴訟法第 1 巻〔第 3 版〕』（2011 年）556 頁〔香城敏麿＝井上弘通〕。その利益考量にあたっては、その一方で、不利益の観点として、①捜査や裁判に対する不当な影響をもたらすおそれ、②被告人、被害者など個人の名誉その他の利益や公序良俗などの社会の利益を損なうおそれ、③関連事件の捜査や裁判に対し不当な影響をもたらすおそれなどが、他方で、利益としては、④憲法 82 条・37 条の定める裁判の公開の要請の充足、⑤被告人など関係人の訴訟活動等を容易にして適正な裁判等に寄与する、⑥他の裁判の資料となるなど公私の必要に応える、⑦国民に正しい情報を提供して理解を不構えるなどの利益が得られることへの期待、などが考えられ、書類の開示法制は、これら両面の利益を調和させるように工夫されなければならない旨が指摘されている。同上 560 頁。

2　人身犯罪の未然防止――ストーカー事案を中心に

(1)「被害者特定事項」の扱い

犯罪被害の未然防止がもっとも強く要求される類型の 1 つが、ストーカー事案である。平成 11 年に発生した桶川ストーカー事件を契機に、この問題の深刻さが認知され、いわゆるストーカー規制法が制定されたことは、ここで改めて述べるまでもない。

ストーカー事案への適切な対処については、事案の性質を的確に把握することのみならず[8]、情報の扱いについても、慎重な取扱いが要請されることも多い。平成 24 年 11 月に神奈川県逗子市で発生した、被害者が元交際相手に自宅で刺殺されたという「逗子ストーカー殺人事件」を例に、この問題を考えてみることにしたい。

被害者は、元交際相手であったストーカー行為者との交際を終了させた後、別の人と結婚して姓を変え、転居もしていた。しかし、当該行為者は、被害者の SNS を特定し、それに基づいて嫌がらせのメールを大量に送信するなどしていた[9]。その後、被害者からの相談に基づき、警察が行為者を脅迫罪で逮捕する際、被害者は「自らの新しい姓や転居先は知らせないでほしい」という要請をしていたものの、逮捕にあたった警察官が当該行為者の前で、逮捕状の関連資料に書かれていたこれらの情報を読み上げていたことが報じられている[10]。

---

8)　ストーカー事案の実態把握や、事案の危険性評価の困難性について、たとえば、青山彩子「警察におけるストーカー対策」刑法雑誌 55 巻 3 号（2016 年）64 頁以下、島田貴仁「ストーキングの被害過程」同 71 頁以下など。

9)　当該事件では、当初はストーカー行為がメールで行われたため、行為当時のストーカー規制法では、その対象行為とすることができないという問題もあり、その後の同法の改正へとつながっている。技術の進歩に法律が迅速に対応する必要性をより如実に示す事案であるともいえる。

10)　平成 24 年 11 月 9 日付各紙夕刊報道。なお、その 1 ヶ月後のストーカー規制法

そして当該行為者は、この脅迫事件で執行猶予付きの有罪判決を受けた後、インターネット上の質問サイトなどにおいて、本来の目的を隠しつつ、被害者の住所を特定するための情報収集をしようと試みた形跡があったほか[11]、探偵事務所に被害者の住所についての調査を依頼し、依頼を受けた探偵事務所において、被害者の居住する市の市役所の納税課に虚偽の問い合わせ電話をして被害者の情報を聞き出すなどして、被害者の居住地の情報収集に努め[12]、その住所を知った直後に被害者宅を訪れ、そこで被害者を刺殺し、自らも自殺した旨が報じられている。

このような問題は、ストーカー事案のみならず、DV 事案等でも発生しうる。このうち住民基本台帳の閲覧に関しては、平成 16 年 7 月 1 日付の総務省自治行政局長通知により、住民基本台帳制度におけるドメスティック・バイオレンス、ストーカー行為等の被害者の保護のための措置が講じられ、平成 24 年 9 月 26 日付の総務省自治行政局長らの通知により一部改正の上、実施されている[13]。だが、報道においては、閲覧制限対象情報である旨の情報の共有が、十分に進んでいなかった実態も明らかにされている[14]。

逮捕時における「被害者特定事項」の読み上げという問題に関連しても、本事件などを契機として、逮捕状のみならず、起訴状、判決書など、刑事手続で利用される書面に被害者の実名が記載され、それが被疑者・被告人に知られる

に基づく警告の際には、被害者の居住地の特定を防ぐため、所轄署長名ではなく県警本部長名でそれを出すといった配慮がなされていたという。平成 24 年 11 月 11 日付産経新聞報道。

11)　平成 24 年 11 月 8 日付読売新聞朝刊報道など。

12)　この探偵事務所から依頼を受けた別の探偵が、被害者の夫を装った苦情電話をガス会社にして被害者の情報を聞き出した行為、被害者の居住する市の市役所の納税課に虚偽の問い合わせ電話をして被害者の情報を聞き出した行為について、前者につき不正競争防止法上の営業秘密侵害罪、校舎につき偽計業務妨害罪の成立が認められている。名古屋地判平成 27 年 1 月 20 日（LEX/DB：25505781）。

13)　総務省「報道資料住民基本台帳制度におけるドメスティック・バイオレンス、ストーカー行為等の被害者の保護のための措置の一部改正」（2012 年）。

14)　平成 26 年 1 月 25 日付朝日新聞報道。

ことにより、同一被害者が同一加害者からさらに被害を受けるおそれが増加すること自体の問題性が意識されるようになった。このうち、逮捕状については、平成 24 年 12 月の警察庁の通達により、被疑事実の要旨の記載にあたり、一方では、犯罪事実の特定、他の犯罪事実との識別を可能にする必要性に留意しつつ、当該事案での再被害防止への配慮の必要性の高さを検討し、「①被疑者に知られていない被害者の氏名ではなく、被疑者が了知している旧姓、著名な芸能人や作家等の通称名等を用いること、②被疑者に知られていない被害者等の住所、居所を記載しない、又は『○○県内において』等の概括的な表記にとどめること等、その表記方法について事案に応じて柔軟に検討する」という取扱いがなされている[15)]。

なお、これらの事件を契機として、平成 28 年のストーカー規制法の改正で、ストーカー行為等をするおそれがある者であることを知りながら、その者に対して、その相手方の氏名、住所等の情報を提供することを禁止する規定が、新たに設けられている[16)]。

また、起訴状や、判決書きについて被害者氏名等の秘匿をすることが許容されるかという論点も、たしかに生じうる。結論的には、訴因の特定（罪となるべき事実の特定と防御対象の提示）に欠けるところがなく、審判対象が確定していると認められるのであれば、必ずしも被害者の実名等の記載は、必須ではないと考えることができる[17)]。

15）石川光泰「再被害防止への配慮が必要とされる事案における逮捕状の請求等について」警察学論集 66 巻 6 号（2013 年）55 頁以下。逮捕状に被疑事実の要旨の記載を要求する法の趣旨を踏まえれば、被害者情報の保護の必要性が特に高い場合に限られよう。その場合、被疑者が元々了知している情報以上の情報を被疑者に与えないという観点を目安に、表示方法を選択すべきとする指摘もある。峰ひろみ「刑事手続における犯罪被害者情報の保護についての一考察」岩瀬徹ほか編『刑事法・医事法の新たな展開（下）町野朔先生古稀記念』（2014 年）493 頁以下。

16）種谷良二「ストーカー行為等の規制等に関する法律の一部を改正する法律について」警察学論集 70 巻 1 号（2017 年）4 頁、高野麿央「ストーカー行為等の規制等に関する法律の一部を改正する法律の逐条解説等について」同 19 頁以下。

17）酒巻匡「被害者氏名の秘匿と罪となるべき事実の特定」岩瀬徹ほか編『刑事法・

(2) 警察との情報共有の限界と GPS 情報の利用可能性

上にみたところからも明らかなように、「被害者特定事項」の秘匿に関しては、刑事訴訟法上の基本原則との調整が必要となる。そのため、ストーカー等による実害結果発生の未然防止という、保護の観点のみで論ずることはできないという問題性が生ずることになる。

さらに、それ以上に問題となるのが、このような被害者側の情報のコントロールのみでは、被害の未然防止にとって、必ずしも十分ではないという事情である。これを、平成 28 年 5 月に小金井市で発生した、芸能活動をしていた女性に対する「ストーカー殺人未遂事件[18)]」を例にみることにしたい。

かねてより、ストーカー行為者（被告人）から SNS 上で執拗な嫌がらせを受けていた被害者は、自宅を管轄する警察署に相談し、緊急事態に即応するため、被害者の携帯電話番号を被害者の自宅住所を登録内容として「110 番緊急通報登録システム」に登録していた。そして、自宅住所とは異なる場所での刺傷行為の発生時に、被害者の携帯電話からの 110 番通報を受けた際、通信指令本部のモニターに登録されていた自宅住所が表示されたため、通報場所の位置情報を確認しないまま、自宅を管轄する警察署に自宅へ向かうよう指示し、結果として、事件現場に警察官が臨場するのが遅れてしまったという事情が存在した[19)]。また、被害者は、ライブハウスに出演するという事件当日の自らの行動について、自宅を所轄する警察署に伝えていたが、当該警察署から事件現場となった警察署への警戒の要請がなされていなかったことも明らかになっている。

これらの事情について、事前に自宅を所轄する警察署から事件現場となった

医事法の新たな展開（下）町野朔先生古稀記念』（2014 年）452 頁以下、小木曽綾「犯罪被害者等および証人を保護する方策」論究ジュリスト 12 号（2015 年）80 頁など。

18)　東京地裁立川支判平成 29 年 2 月 28 日（裁判所ウェブサイト）。

19)　平成 28 年 5 月 25 日付各紙報道。

警察署との間に、仮に情報の共有がされていたとして、果たして、この事件を確実に防止することができたかについては、「たられば」の仮定の話でしかないが、そう断言することは必ずしもできないように思われる。だが、京都市に居住していたストーカー行為者が、小金井市の事件現場（ライブハウス）に向かっていたことを、少なくとも被害者が覚知することができ、被害者が覚知した情報を警察との間で共有できていたのであれば、被害者自身および警察側においても、的確な対応をより確実に講ずることができた、という意味において、事件を未然防止できた可能性が相対的に高まっていたと述べることは、許されるであろう。

なるほど、本件では、ストーカー行為者に対して、ストーカー禁止法上の警告や禁止命令は発せられていなかった。だが、仮に禁止命令が行為者に発せられていたとしても、現行法では、それを担保する手段としては、禁止命令に違反した場合の処罰規定があるものの、このような事後的処罰以外の手段は制度的には確保されていない。

そのため、現状では、被害者の安全の確保のためには、①被害者自身が「逃げる」「加害者にその所在を知られないようにする」か、②逮捕等により加害者自身の身体を拘束するしかないことになる。だが、①これでは、被害者側にとっては、その社会生活に多大な制約・負担が課せられるだけでなく、十分に不安を払拭することができないことになる。その反面、②加害者側にとっても、身体拘束を伴うのであれば、その権利自由への制約も非常に大きなものとならざるを得ないというディレンマを抱えることになる[20)]。

近年になって、ストーカー事案に関して、加害者の位置情報を収集するために GPS 端末を利用する可能性が指摘されることもある[21)]。その場合、たとえば、

20）安田貴彦「犯罪被害者支援の現状と今後の課題」井田良ほか編『新時代の刑事法学下巻――椎橋隆幸先生古稀記念――』（2016 年）432 頁。

21）警察庁の犯罪被害者等施策推進会議の決定に基づく「第 18 回基本計画策定・推進専門委員等会議」では、川出敏裕構成員により、「DV 防止法の接近禁止命令とかストーカー規制法の禁止命令等の担保手段として、被害者に近づいてはいけないと

現行のストーカー規制法の定める公安委員会という行政機関により発せられる禁止命令に加えて、被害者への接近禁止等を内容とする、DV 防止法の保護命令（同法 10 条）のような裁判所による命令制度を設け、裁判所の審査に基づいて、加害者に対する電子監視（GPS 監視）を命ずる可能性も検討に値する。そして、それは、被害者の安全の確保のために行われるものである以上、行為者の位置情報は、原則として被害者のみが知れば十分なのであるから、緊急を要する場合を除いて警察等が位置情報を知ることはないという制度設計とすれば、警察が被疑者の位置情報を知ることを目的とした、いわゆる GPS 捜査における被疑者に対する法益侵害[22]よりも、行為者に対する法益侵害の程度は軽いと考えることもできるように思われる。のみならず、このような措置は、加害者の身柄拘束という対応に比べても、加害者側の負担ははるかに軽くなり、被害者のより確実な安全確保との相関においても、権利自由の制約の程度はかなり低いと評価する余地は十分にあるように思われる[23]。

いうことを確保するために電子監視を導入するということであれば検討に値するように思います。さらに、先ほどの法務省からのご回答によれば、保護観察の遵守事項として、被害者に近づいてはいけないということが設定されているということでしたので、その担保手段としての電子監視というのも考え得るかなと思います。再被害防止のために警察の方がパトロール等をされるということでしたが、そうはいっても 24 時間ずっと見ているというわけにはいかないでしょうから、それに代替する一つの手段として考え得るのではないでしょうか。もちろん、行政命令の担保手段、あるいは遵守事項の担保手段としての電子監視というのが法制度上どのように位置付けられるのかといった問題はありますが、検討事項の一つとして考えていただければと思います」という見解が示されている <https://www.npa.go.jp/hanzaihigai/sakutei-suisin/kaigi18/gijiroku.html>。

22） なお、最大判平成 29 年 3 月 15 日（裁時 1672 号 1 頁）参照。

23） 安田・前掲注（20）論文 432 頁参照。

3 「犯行ツール」等の対策と本人確認制度等に基づく犯罪の未然防止

(1) 銀行取引等における本人確認制度などの機能

犯罪被害の未然防止のためには、罪種によっては、犯罪に用いられることの多い「犯罪ツール」についての対策を講ずることも重要となる。

たとえば、平成 15 年頃から、刑事政策上の最大の課題であり続けている「振り込め詐欺」をはじめとした特殊詐欺においては、架空人名義や他人名義の銀行口座、および携帯電話等が犯行に使われるツールとして重要性を帯びている。そのため、これらを規制することが、特殊詐欺のみに限られるものではないが、一定類型の犯罪の防止にとって重要な意義を有することになる。

その際の規制内容の柱の 1 つをなすのが、本人確認である。

銀行口座に関する本人確認は、かつては、大蔵省（現財務省）の通達に基づいた、本人確認と取引記録の保存が要請されていたに過ぎず、当然のことながら違反に対する制裁もない状態が続いていた。これに対して、テロ資金供与防止条約を国内的に担保するための法整備として、平成 14 年に「金融機関等による顧客等の本人確認等に関する法律」（「本人確認法」）が制定される。そして、政府間機関である FATF（Financial Action Task Force on Money Laundering・金融活動作業部会）による改訂勧告（平成 15 年）に基づく形で、新たに「犯罪による収益の移転防止に関する法律」（「犯罪収益移転防止法」）が制定されるに至っている[24)]。同法 4 条では、金融機関等の特定事業者（同法 2 条）に、一定の取引を行う際の本人特定事項の確認（本人確認）を行う義務を課し、顧客等が本人特定事項を偽った場合についての罰則が設けられている（同法 25

24)　これに伴って、本人確認法は廃止された（犯罪収益移転防止法附則 2 条）。以上について、犯罪収益移転防止制度研究会編著『逐条解説犯罪収益移転防止法』（2009 年）6 頁以下。

条)。

以上とならんで、犯罪収益移転防止法の枠組みでは、疑わしい取引があった場合の、金融機関等の特定事業者による行政庁への届出義務（同法 9 条）や、届出を受けた国家公安委員会による捜査機関等への情報提供等の制度（同法 11 条）によって、捜査機関が、必要な情報を得ることができる仕組みが設けられている。

(2) 携帯電話事業等における本人確認制度および情報の取り扱い

また、携帯電話については、平成 17 年に「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」(「携帯電話不正利用防止法」）が制定されている。これは、当時、特殊詐欺において本人確認が徹底されていない携帯電話が利用されることが多く、その名義人から直接犯人にたどり着くことが困難となり、捜査上の支障が生ずる反面、こういった匿名携帯電話が容易に入手可能な状態にあり、特殊詐欺の被害が急速に拡大する大きな要因にもなっていたという背景に基づいて制定されたものである[25]。同法は、携帯事業者に、役務提供契約を締結する際に、運転免許証の提示等により本人特定事項の確認（本人確認）を行う義務を課し、契約の相手方が本人確認事項を偽った場合についての罰則が設けられるなど、犯罪収益移転防止法と同様の枠組みが設けられている[26]。

さらに、携帯電話不正利用防止法では、契約者確認に関する制度も設けられている。同法 8 条は、警察署長が、携帯電話が不正に利用されていると認める

25)　親家和仁「『携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律』について」警察学論集 58 巻 8 号（2005 年）53 頁。

26)　さらに、自己が契約者となっていない携帯電話の譲渡や匿名貸与営業、さらにはそれらの勧誘・誘因行為についても、罰則を伴う禁止行為とされている。同法 21 条、10 条および 22 条。

に足りる相当な理由がある場合に、携帯電話の役務提供契約を締結した事業者に、当該役務提供契約にかかる契約者について、役務提供契約上の地位を有している旨の確認（「契約者確認」）を行うことができることを定める。これは、犯罪被害の拡大防止の観点からは、犯罪に使用された思われる携帯電話について、それを即座に利用停止することが、憲法で保障された表現の自由、通信の秘密との関係、犯罪に利用されたことの認定に伴う諸問題からできないため、それに代わる方法として、改めて契約上の地位の確認を行い、それが確認できないときは役務提供を拒否できる（同法 11 条）という仕組みとして設けられたものである。携帯電話の犯罪利用実態をもっとも知悉しているのが警察署長であることから、警察署長からの求めにより契約者確認ができることとされている[27]。

(3) 古物営業等における本人確認制度および情報の取り扱い

また、近年、インターネット・オークションをはじめとする商品転売が容易かつ高価に行われる仕組みが整備されてきたことにより、店頭から商品を盗み、それを転売して金銭を利得する行為が拡がっているように思われる。店頭からの商品の窃取は、いわゆる「万引き」と称される行為類型であるが、こういった類型は、思春期等の逸脱行為や出来心で行われる万引きとは異なる形での被害防止、すなわち盗品の転売を抑制する仕組みが必要となる[28]。

昭和 24 年に制定された現行の古物営業法は、古物の買い受け等をする際には、当該相手方の住所、指名、職業および年齢を確認し、不正品の疑いがある場合には、ただちに警察にその旨を申告しなければならない旨を定める（同法 15 条）。これは、古物商が犯罪の防止に協力する上でもっとも重要なのは、盗品を取り扱わないことであり、古物商が慎重な態度で臨むことで盗犯が減少し、

27)　親家・前掲注（25）論文 63 頁以下。

28)　なお、バイクに関しては、日本二輪車普及安全協会の運営する「二輪車盗難照会システム」がある。

疑わしい場合に警察に対して積極的な協力がなされれば、検挙も著しく向上するという考えから、このような制度が設けられたと説明されている[29)]。

同時に、警察の側としては、必要があると認める場合には、古物商または古物市場主（古物商等）に対して、盗品等の品触れを発し、これを受けた古物商等には、それを 6 か月保存し、その間に当該古物を所持、受け取り、または、古物市場に出た場合には、その旨を警察官に届け出る旨の義務が定められている（同法 19 条）。

そして時代が下り、先にも述べたように、インターネット・オークションを介した古物取引きが盛んに行われるようになった昨今の状況に対応する形で、平成 14 年の古物営業法の一部改正により、古物競りあっせん業に関する規定が新設された。

インターネット・オークションサイトを運営する古物競りあっせん業者は、古物の売却をしようとする者から出品を受け付けようとするときには、その出品者の真偽を確認するための措置をとるよう務めなければならない旨が定められている（同法 21 条の 2）。ただし、古物競りあっせん業者は、自らが売買の当事者や目的物を直接見聞するわけではなく、また、インターネット・オークションでは、盗品等ではない物品が大量に取り引きされていることなどから、出品者の確認は、努力義務とされた。また、記録の作成および保存についても、同様の理由から努力義務とされている（同法 21 条の 4）。

他方で、古物競りあっせん業者には、出品された古物に盗品等の疑いがあると認めるときに、ただちに、警察官にその旨を申告する義務が課されている（同法 21 条の 3）。盗品等の速やかな発見を図るため、一定の範囲で申告が義務付けられているわけである。

さらに、警察の側に対しては、出品された古物について、盗品等であると疑うに足りる相当な理由がある場合には、警察本部長等が、古物競りあっせん業者に対して、当該古物にかかる競りの注視を命ずる制度が設けられた（同法

29)　間狩信義＝横井克己『古物営業法解説』（1949 年）102 頁以下。

21 条の 7）。また、同じく警察本部長等は、必要があるときは、古物競りあっせん業者から盗品等に関し、必要な報告を求めることができるとされている（同法 22 条 3 項および 4 項）。これは、古物営業法の施行のためには、競りの中止の命令を実施するための古物競りあっせん業者の体制に関する事項や、当該命令に従い競りを注視する義務等の古物競りあっせん業者の義務の履行状況等について把握する必要があるために設けられた、一般的な報告徴収の規定と位置づけられている[30]。

4　街頭犯罪の防止と情報の共有

（1）即応体制整備のための情報共有

街頭設置の防犯カメラは、捜査の端緒として、きわめて重要な意味を有するに至っている。警察庁によれば、平成 28 年の、いわゆる「余罪」を除いた刑法犯の検挙件数 22 万 318 件のうち、防犯カメラが被疑者特定の端緒となった件数が 1 万 2994 件で、検挙件数の 5.9％を占め、職務質問の 20.9％、被疑者・参考人の取り調べの 8％に次ぐ、第 3 位であった。そして、ひったりくりで防犯カメラ映像が被疑者特定の端緒となったのが 20.4％、すりで 12.3％、強盗で 10.8％となるなど、街頭犯罪の検挙にとって犯罪捜査支援機能を果たしているのが実態となっている[31]。このような捜査の端緒を得るものとしての防犯カメラの利用は、直接的な意味の防犯ではないが、被疑者の早期の特定・検挙は、間接的に防犯にも寄与しうるものともいえる。

街頭防犯カメラの設置主体は、様々である。警察が直接に設置しているのは、平成 28 年 3 月末現在で、26 都道府県で合計 1,530 台である[32]。もちろん、そ

30）　以上について、友井昌宏「インターネットを利用した古物取引の安全の確保」時の法令 1691 号（2003 年）27 頁以下。
31）　平成 29 年 1 月 19 日付読売新聞夕刊報道。
32）　警察庁編・前掲注（4）書 112 頁。

れをはるかに上回る数の街頭設置カメラが、行政や、特に民間部門によって設置されていることは、周知のところである。

近年、大阪府では、自治体の設置した防犯カメラについて、大阪府警が画像を確認する場合には、捜査関係事項照会書を提出のうえ、設置場所において自治体の担当職員により SD カードなどの記録媒体を取り出すという運用をしている。だが、夜間や休日などには、自治体職員による対応ができないため、初動捜査に支障が生ずる例が生じていた。そこで、平成 25 年 9 月以降、大阪府警の各警察署長が管轄する自治体との間で、自治体設置の防犯カメラについて、自治体職員による対応ができない夜間や休日の緊急を要する犯罪捜査において、Wi-Fi により接続されたカメラにつき、協定に定める画像管理責任者等である警察署長等の指揮を受けた警察官が、警察が自治体から貸与を受けた専用の端末を近づけて映像をダウンロードして入手し、事後すみやかに、自治体に対して、事件の概要や映像の内容などを記した照会書等の提出し承認を得るほか、貸与にかかる専用端末に記録される抽出履歴を定期的に自治体に提出する旨の協定が締結されている。平成 29 年 1 月現在で、20 自治体との間で協定が締結され、約 3000 台のカメラがこの協定にかかるものとなっている[33]。このような取り組みにより、現実に、夜間に発生した街頭犯罪等の初動に効果がある旨も報じられている[34]。この場合、画像の抽出履歴を定期的に自治体に提出することで濫用防止を図るほか、抽出した映像自体は犯罪捜査に関するものであるから、公安情報として、行政機関個人情報保護法の開示対象からの除外（同法 14 条 5 項）や行政機関情報公開法の公開対象からの除外（同法 5 条 4 項）はなされるものの、この抽出履歴自体は、情報公開の対象となりうるものと考えられる。このような手段を講ずることによって、当該協定に基づく運用の適正性と透明性とが図られているとの評価が可能である。

以上とは異なる目的・文脈において、警察と自治体との間で防犯カメラ映像

33)　大阪府犯罪抑止戦略本部「自治体が運用する無線通信式防犯カメラの活用による迅速な捜査の推進について」（2017 年）。

34)　平成 29 年 2 月 16 日付朝日新聞夕刊大阪版報道。

の共有に関する協定が締結される例もみられる。平成 29 年 1 月 22 日には、警視庁と足立区との間で、「足立区テロ及び災害対策事業の推進に関する覚書」が締結された。その一環として、足立区の設置する 70 台（平成 29 年度からは 100 台）の災害用定点カメラの映像を、テロや災害などによる非常事態が発生した場合に限り、警察・消防がライブ映像を閲覧できるようにするという仕組みが導入されている。この場合、プライバシーに配慮して画像は録画しないこととされているようである[35]。

これらは、情報共有の目的の相違に応じて、当該目的を達成するために必要な形態でのカメラ映像の情報共有と、それに対する透明性の確保を図ろうとする枠組みであるということができる。

(2) 防犯カメラ映像の利用方法――犯人検挙と犯罪の未然防止

これに対して、民間部門で設置された防犯カメラ映像について、近時、設置者自身が、カメラ映像を店頭やインターネット上に公開するといった手段を用いて、被害品の回復や犯人の検挙等を自らの手で図ろうとする動きが、しばしば生じている。

平成 26 年 8 月には、東京・中野の有名古書店が、販売価格 27 万円のブリキ玩具を万引きした犯人と思われる者の防犯カメラ映像をモザイク処理を施したうえで、「1 週間以内に返しに来ない場合は顔写真のモザイクを外して公開します」とのメッセージとともに自店の Web サイト上で公開するといった事態が生じ、当該行為の是非に関して物議をかもした[36]。また、平成 29 年 2 月に

35)　平成 29 年 1 月 27 日付産経新聞報道。

36)　その後、当該古書店は、警察からの要請に応える形で写真の公開を止め、当該 Web を削除した。平成 26 年 8 月 13 日付朝日新聞朝刊報道など。そして、警察の捜査に基づき当該犯人は逮捕、起訴され、公判では、損害の一部弁償として被害店舗に 10 万円を支払っていることなどが考慮され、懲役 1 年、執行猶予 3 年の刑が宣告された。東京地判平成 26 年 10 月 31 日（LLI/DB：L06930600）。

は、千葉県のコンビニエンスストアが、客の顔が映った防犯カメラの画像に「万引き犯です」旨を書き添えたうえで、それを店内に約2週間貼り出していた、という事案を嚆矢として、防犯カメラ画像の「公開」に関して、適切さが問われるような事案についての報道が相次いだ[37]。

こういった事象は、映像データの適切な利用という観点からみると、結論としては問題が残るといわざるをえない。種々指摘されているように、こういった行為には、恐喝罪（脅迫罪）や名誉毀損罪[38]（さらに不法行為法上の名誉毀損）の成立の可能性も考えられないわけではない。また、その場合、刑法の典型論点である「権利行使と財産犯」の応用問題ともなりうるが、当該行為が、社会通念上相手方に受忍を求める限度を超えないものでない限り、自救行為（自力救済）としての違法性阻却もされないであろう[39]。

犯罪が発生した後の犯人の検挙や被害品の回復等については、法執行機関や司直の手によるのが原則である以上、当該防犯カメラ映像の利用についても、警察への提供ということ以外には、原則として適法とされる余地はないということになる。

だが、これに対して、犯罪被害拡大の未然防止については、店舗側が自ら行うものであるし、そのことが期待されることになる。それゆえ、窃盗犯人の画像について、それを、再被害防止のために使うことは、防犯活動の一環として、社会的にも許容され、また防犯カメラの設置趣旨にも合致するものと考えられる。

なお、近時の防犯カメラ映像の高精細度化に伴い、旧来のアナログ方式のカメラではなく、いわゆるIPカメラ等により得られる鮮明なデジタル画像については、原則として個人情報に該当するものとして考えるべきである[40]。その

37）これらの一連の動きについて、平成29年2月20日付産経新聞報道など参照。
38）広島高判昭和30年2月5日（裁特2巻4号60頁）参照。
39）最決平成元年7月7日（刑集43巻7号607頁）参照。
40）拙稿「街頭設置カメラの高機能化・生体認証機能と個人情報該当性―改正個人情報保護法と防犯カメラ条例の意義―」法学会雑誌57巻2号（2017年）218頁以下。

場合に生ずる個人情報保護法上の論点については、以下の 6 において、改めて検討することとしたい。

5　出所情報の通知・共有

さらに、犯罪による再被害防止においては、受刑者の出所情報についての利用という枠組みが存在する。

平成 13 年 1 月に、法務省刑事局長通達により、「被害者等通知制度実施要領」が改正されるとともに、刑事局長・矯正局長・保護局長の連名による通達が発せられ、被害者等に対して、刑務所からの犯人釈放に関する「出所情報」を通知する制度が導入された。これは、かねてより被害者等により表明されていた、犯人の出所情報を知りたいとの要望に応える形で実施されたものである[41)]。

通知される情報は大きく 2 つであり、①釈放前における、自由刑の執行猶予終了予定時期等と、②釈放後における、仮出所または自由刑の執行終了による釈放の事実および釈放年月日等である。出所情報の通知制度の目的は、被害者その他の刑事事件関係者に対し、受刑者の刑務所からの釈放に関する情報を通知することにより、刑の執行等について、被害者を始めとする国民の理解を得るとともに、刑事司法の適正かつ円滑な運営に資することにある[42)]。

その後、同年 10 月には、被害者等が同じ犯人から再び被害を受けることを防止し、その保護を図るため、受刑者の釈放等に関する情報を通知・通報する制度が導入された[43)]。この制度の背景をなすのは、(1) 被害者にとってみれば、

41)　田野尻猛「被害者等に対する出所情報の通知の実施について」刑政 112 巻 4 号（2001 年）50 頁。

42)　同上 52 頁。

43)　同制度の概要について、杉山徳明「再被害防止のための出所情報通知・通報制度について」罪と罰 39 巻 2 号（2002 年）75 頁以下。以下の制度の概要についての説明も、同論文による。

事案によれば、出所後に報復されるのではないかと不安を抱く場合があることは、きわめて自然であること[44]、(2) 当該犯人からの再被害が具体的に予想され、被害者等が転居する等の再被害防止のための措置を講ずる必要がある場合に、出所情報を得ることはきわめて重要であること、(3) 再被害を防止するには、単に被害者に出所情報を通知するだけでは不十分で、警察において適切な対応を講ずる必要が生ずることもある、といった諸点である。他方で、(4) 出所情報が開示されれば、受刑者の改善更生やプライバシーに影響を与えることになるため、その点を考慮する必要がある。

以上に基づき、一方では、被害者の再被害防止・保護の要請、他方で、受刑者の改善更生・プライバシーの保護の要請とを合理的に調整し、同時に法務省の関係機関と警察との間で十分な協力体制がとられるよう配慮する形で、①検察官から被害者に対し、受刑者の釈放予定に関する通知を行う制度と、②行刑施設および地方更生保護委員会から警察に対し，受刑者の釈放に関する通報を行う制度という、2 つの制度が導入された。

①に関しては、希望する被害者等に対して通知を行うものであるが、受刑者の改善更生の利益に配慮して、通知する情報について、まず、ⓐ釈放予定時期について、原則として月の上旬・中旬・下旬のみを通知することとし、被害者等と加害者との接触回避等のための措置を講じるために必要不可欠な場合にのみ釈放予定日を通知することとされている。またⓑ帰住予定地については、原則として通知しないが、被害者等と加害者との接触回避等のための措置を講じるために特に必要な場合にのみ、都道府県名あるいは市区町村名までを通知し、帰住先が被害者等の住居地と近接している場合にかぎり、町字名まで通知する。

②に関しては、行刑施設、地方更生保護委員会または保護観察者から警察に対して通報を行うという、行政機関相互の協力措置である。行刑施設等は、通報の要請があった受刑者について、警察に対する通報を行うのが相当であると

44)　なお、平成 9 年には、強姦罪で服役後、強姦被害を訴えた被害者を出所直後に探し出し殺害するという事件が発生しており、当該被告人には、死刑が宣告されている。最決平成 16 年 10 月 13 日（裁判集刑 286 号 357 頁）。

認めるときに、ⓐ釈放予定時期とⓑ帰住予定地等を通報することができる。通報を受けた警察では、それを基に再被害防止措置を講ずるとともに、通報を受けた情報を被害者等に対して教示する際には、前述した検察官が被害者に通知する場合と同様の配慮を行うこととなっている。

そして、警察においては、「再被害防止要綱」（平成 19 年 6 月 11 日付警察庁刑事局長等通達）」に基づき、同じ加害者により再び危害を加えられるおそれのある犯罪被害者等を再被害防止対象者に指定し、再被害防止のための関連情報の収集、関連情報の教示・連絡体制の確立と要望の把握、自主警戒指導、警察による警戒措置、加害者への警告等の再被害防止措置を、関係機関との連携を図りつつ、講じている[45)]。

さらに、それに先立つ平成 17 年 6 月からは、「子ども対象・暴力的性犯罪の出所者情報の共有」を、警察庁による通達に基づいて行っている。これは、アメリカの「メーガン法」に代表されるような性犯罪者の再犯防止対策が立法化されていないなか、現行法下で実施可能な行政機関相互の情報交換の範囲内で行うものとされている[46)]。

6　犯罪被害拡大防止・再被害防止と個人情報保護法

（1）犯罪被害の防止における情報の重要性

ここまで、犯罪被害の防止を図る制度、取り組みにおける情報の扱いについて、思いつくところを縷々述べてきた。以上で検討したもの以外にも情報の扱いの規制、あるいはより迅速で的確な積極的利用が求められる場面は多く存在すると思われる。だが、以上で検討したところだけでも、情報の的確な取扱いと関係機関における必要十分な情報共有が重要となりつつある現状を、不十分

45）　国家公安委員会・警察庁編『平成 28 年版犯罪被害者白書』（2016 年）42 頁。
46）　詳細に関して、たとえば、上野正史「警察における性犯罪対策～子どもに対する犯罪への対策を中心に」警察政策研究 13 号（2009 年）28 頁以下。

ながらも明らかにし得たと思われる。

これらの情報に、個人情報保護法の対象となる情報が含まれていないのであれば、そういった局面での法的規制の問題は生じない。もちろん、そういった情報の不適切な取扱いがなされることで、当該事象に関連する捜査や裁判、あるいは関連する事件の捜査や裁判に不当な影響をもたらすことがあってはならない。それは、主として刑事訴訟法による規制の対象となり得る[47]。その典型が、サイバー攻撃・サイバー犯罪等において、被疑者に関する情報が得られないものの、それに関連した再被害の防止に有益な情報を、刑事訴訟法 47 条に抵触しない範囲で行う、という枠組みである[48]。

(2) 犯罪の検挙という文脈における個人情報の利用

だが、犯罪被害防止のために使う情報というものを考える際には、それは、犯罪行為者（加害者）と対象者（被害者)、さらにはその関係者といった者を中心とした個人情報に該当する情報である場合が圧倒的に多いと思われる。さらに、防犯カメラ映像についても、すでに述べたように近時の高画質化により、原則として個人情報として考えるべきことになっているため、個人情報に該当する情報が、ますます増加している状況にある。

これら個人情報を、被害防止のために利用するにあたっては、まずは、①個人情報保護法の許容する枠組みの中において許容される態様でなければならないことは、言うまでもない。これを、先に簡単にみた、店頭犯罪の文脈で考えてみることにしよう。通常よくみられる、何らかの犯罪被害に遭った店舗が、当該犯罪の証拠となりうる映像とともに警察に届け出る行為、すなわち、当該個人情報の警察への提供は、当該防犯カメラの設置について定められた目的に即した、本来的な利用であると理解できる。もっとも、第三者提供を行うとい

47)　前掲 63 頁および 67 頁。
48)　また、不法行為責任や国家賠償責任を生じさせないという観点も基準となろう。

う利用目的で取得した個人情報の第三者提供は、その利用目的の一態様であるから、個人情報保護法 16 条の利用目的による制限の枠組みにおいて許容されることになりそうであるが、第三者への提供に関しては、同法 23 条の第三者提供の制限規定が、同法 16 条の特則として位置づけられる[49]。そのため、同法 23 条 1 項 1 号または 2 号により、許容されることになると解される。これに対して、窃盗犯人の顔画像をインターネット上に公開するという形で「第三者提供」をする場合も、同条 2 項の「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」という、第三者提供の例外にあたるとする解釈も、論理的には成立しえないわけではない。だが、すでにみたように、このような行為については、それを許容するという社会的合意はなく、むしろ、近代法治国家では許容されない自力救済にあたる可能性、あるいは、名誉侵害等の違法な結果を生じさせる可能性がきわめて高いものである。

このことに典型的に示されているように、防犯カメラ映像等を含めた、犯罪の防止や検挙に関連しうる個人情報の利用については、単に個人情報保護法上許容されるか否かだけではなく、②他の法令との関連においても許容されるか否かを検討する必要もある。とりわけ、関連性を有する蓋然性が高いのが、民法上の不法行為責任を生じさせるか否かであろう。

(3) 犯罪の再被害防止という文脈における個人情報の利用

他方で、これもすでにみたように、犯罪被害の防止は、むしろ当該法益主体の手によってなされることが期待される事項であるといえる（要するに、「戸締まり用心」）。さらに、たとえば、組織的・常習的な窃盗犯人について、当該犯人によるさらなる犯罪被害防止（再被害防止）についても、犯罪被害防止の

49) 園部逸夫編『個人情報保護法の解説〔改訂版〕』（2003 年）144 頁、岡村久道『個人情報保護法〔新訂版〕』（2009 年）241 頁、宇賀克也『逐条解説個人情報保護法〔第 5 版〕』（2016 年）155 頁。

一環として位置づけることができる。

そこで、その目的、すなわち、再被害発生防止の目的で、当該対象者の従前の犯罪行為等の映像などから抽出した個人情報を利用することを例にとって考えてみよう。まず、①個人情報保護法上の枠組みで考えると、防犯目的で取得した情報であれば、それを、自ら防犯目的で利用するのであれば、利用目的による制限原則の範囲内で許容される利用の仕方である。また、それによって、対象者について２度目以降の来店があった場合に、通常の客とは異なる形で、店舗側が警戒を行うことも、最終的には程度問題という面も残るであろうが、②少なくとも「声かけ」等の対応をするといった態様であれば、プライバシーに対する不当な侵害であると評価されることはない。

他方で、組織的・常習的な窃盗犯であれば、近隣の他の店舗等で同種行為を行う可能性が高い。そこで、地域防犯という観点で、当該情報を他店舗に提供するという枠組みの如何について考えてみよう。その場合、提供先が、同一法人内の他店舗であれば「自らの利用」ということになり、上記の例と基本的に異なるところはない。しかしながら、近隣店舗や同一ブランドの店舗でも別のフランチャイジーであれば、他法人であるから、①個人情報保護法上は、「第三者提供の制限」原則のもとで許容されるか否かを判断すべきことになる。この場合、対象者の事前同意を得ること（オプトイン）はまず考えられないので、同条１項１号ないし４号（とりわけ２号）に該当するのでなければ、第三者提供はできないことになる。他方で、たとえば、商店会加盟店や、近隣の同業他社、他行他社の間で、防犯に関する情報を共同利用するという枠組みを作り、そこで対応するのであれば、同条５項３号の共同利用の枠組みとして、個人情報を含む防犯情報の共同利用を行うことは可能となる。だが、個人情報保護法上明らかになるのはここまでで、②いかなる防犯情報を、どの範囲で共同利用することが許容されるのか、については、やはりプライバシーに対する侵害の程度が大きく、共同利用の必要性や合理性との間での比較衡量において許容されないか否か、という不法行為責任を中心とした、個人情報保護法以外の枠組みでの判断が必要となる。

同様の事情は、顔認証機能等の生体認証機能の利用の可否という問題にもかかわる。生体認証機能のついていないプレーンなカメラシステムにおいても、個人が容易に識別可能であれば、当該映像は個人情報である。それゆえ、生体認証機能システムにおいて用いられる対照データ（データベース登録データ）や、それに基づいた認証がなされる映像データも、すべて個人情報であることになる。そのため、高精細であるがプレーンなカメラシステムにより得られた映像を、㋑人間が記憶して常習的窃盗犯等を識別することも、㋺認証機能システムを用いて識別することも、その作業の意義自体は同一であるようにも思われる。だが、①個人情報保護法上は、記憶であれば保有個人データではないのに対して、認証のためのデータベースに登録された情報はそれにあたりうる。また、それとも関連するが、②人間の記録力や目視の限界等と認証機能の精度との相違に起因する識別の精度の問題などを考えると、プライバシー等に対して与える影響は同一ではない。

もちろん、㋺生体認証のために登録される、個人識別符号を含めたデータベース上の個人データについても、個人情報保護法上の個人情報、個人データ、保有個人データに関してそれぞれ設けられる諸原則に則った取扱いをするのであれば、個人情報保護法上は、その利用が禁止されるわけではない。だが、それ以上に、②プライバシーに対する影響に差が生ずるのだとすれば、どの範囲でそれが許容されるかについては、広く世間一般の了解事項も踏まえた上での、比較衡量に基づく判断が必要となる。それゆえ、設定される利用目的の合理性と利用目的の達成に必要な範囲の設定等の個人情報保護法上の解釈問題を踏まえつつ、どの場合に許容されるかについて、犯罪被害の防止という文脈を対象とした、個人情報取扱いのガイドラインを設けることが必要となると考えられる。

(4) 情報の適正な利用・共有を促す枠組みの必要性

個人情報保護法に関しては、その制定時、法制定により、それまでの社会一

般の意識を改め、個人情報を保護する文化の醸成が期待された一方、現実には期待以上の結果を招くことになり、ともすれば、「個人情報にあたるのであれば使ってはいけない」といった誤解が生ずる結果となった側面がある[50]。

それは、行政機関にあっても例外ではなかったように思われる。これを、2では論じなかったが、ストーカー事案と並んで人身に対する犯罪の防止として重要な課題である、児童虐待防止法を例にとり、検討することにしよう。平成19年の児童虐待防止法の一部改正で、行政機関、学校、医師などの関係者は、市町村や福祉事務所の長、あるいは児童相談所長から児童虐待に関連する資料や情報の提供を求められた場合、「当該資料又は情報について、当該市町村長、都道府県の設置する福祉事務所の長又は児童相談所長が児童虐待の防止等に関する事務又は業務の遂行に必要な限度で利用し、かつ、利用することに相当の理由があるときは、これを提供することができる」とする規定が設けられた（児童虐待防止法13条の4〔現行〕）。

児童虐待に関連する資料ないし情報には、当然のことながら、虐待者や被虐待者などを中心とした個人情報が、原則として含まれていることになる。もちろん、現在の個人情報保護法の枠組みにおいても、児童虐待防止のために当該個人情報を第三者に提供することは許容される。すなわち、①それが行政機関の保有する個人情報の場合、ⓐ当該児童虐待事案への対応のために収集された個人情報であれば、本来の目的のためのものとして、利用および提供することができ、共有することが可能となる（行政機関個人情報保護法8条1項）。これに対して、ⓑ当該目的以外に行政機関が保有している当該事案に関連する個人情報を児童虐待の防止という目的外の利用をする場合でも、「保有個人情報を提供することについて特別の理由」があるのであれば、当該情報を提供、共有をすることができる（同法8条2項4号）。また、②民間組織が保有する個人情報であれば、個人情報保護法23条2項または3項により、本人の事前の同意がなくても、当該情報を第三者に提供することができる。

---

50)　関啓一郎『ポイント解説平成27年改正個人情報保護法』（2015年）1頁以下。

しかしながら、公務員の守秘義務との関連も含めて「これまでも、児童虐待に関係する機関では、必要に応じて情報交換等がなされてきたところであるが、ややもすると個人情報保護等を過大に重要視し、必要な情報提供（交換）にさえも躊躇するケースも散見され」る状況が生じていた。そのことから、必要な情報が適切に提供され、児童虐待防止対策に役立てることを目的として、この規定が設けられたものである[51)]。

また、平成 28 年に成立した再犯の防止等の推進に関する法律においても、その 5 条において、国、地方公共団体は、それら相互の連携、および民間団体等との緊密な連携協力の確保とならんで、「再犯の防止等に関する施策の実施に当たっては、再犯の防止等に関する活動を行う民間の団体その他の関係者に対して必要な情報を適切に提供する」ものとされ、他方、それにより個人情報の提供を受けた民間団体等は、それを「適切に取り扱わなければならない」とする規定が設けられていることも注目される[52)]。

(5) 小　括

犯罪の未然防止等のために個人情報を利用しようとする場合、とりわけ加害者側の情報については、その収集や利用に関して、加害者本人の「同意」を得ることが基本的に考えられない。そのため、個人情報保護法制における個人情報の利用の枠組みにおいては、犯罪の未然防止のための利用は、「原則的に禁止されるが、例外的に許容される場合にあたるか」という観点で検討せざるを

51)　菊澤信夫「児童虐待防止法等の改正及び児童虐待防止に向けた取組について」警察学論集 60 巻 10 号（2007 年）166 頁。関係機関における連携の不足や情報を共有する仕組みが確立していないことが、児童虐待の防止にとって問題が大きいことは、かねてより指摘されているところである。厚生労働省・社会保障審議会児童部会児童虐待等要保護事例の検証に関する専門委員会『子ども虐待による死亡事例等の検証結果等について（第 3 次報告）』（2007 年）53 頁以下、岩井宜子「児童虐待防止法改正の意義と課題」刑事法ジャーナル 10 号（2008 年）91 頁。

52)　なお、川出敏裕「これからの犯罪対策」法学教室 438 号（2017 年）1 頁参照。

えなくなる。そのことは、個人情報の利用を図りつつも、同時に「個人の権利利益を保護することを目的」とする以上、個人の同意を得ない形での情報の利用が、「原則として」権利利益の保護に資さないことになる構造となる以上、当然の帰結であるとはいえる。

だが、犯罪の未然防止は、当該被害者にとってはもちろんのこと、加害者側にいる者に、犯罪をさらに重ねることや、再犯を思いとどまらせることで、その刑事責任の拡大を防ぎ、社会への再統合を促すという意味において、社会的な利益という文脈における「豊かな国民生活の実現に資するもの」（個人情報保護法１条）というべきである。そのため、個人情報保護法制上は「例外」ではあるものの、どのような利用ができるのかを、「原則」という観点から定めた法律やガイドライン等が必要となるのである。これは、まさに、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」という同法の目的を実現するために不可欠な要因であるといえよう[53)]。

むすびに代えて

本稿では、犯罪の未然防止という文脈における、必要な施策のあり方と、それに伴う情報の取り扱いについて、縷々検討を加えてきた。繰り返しになるが、それは、思いつくままに行っただけの不十分なものでしかない。だが、そのような検討結果からも、少なくとも、犯罪被害の未然防止の要請が高まる中、個

53)　なお、平成27年の改正個人情報保護法により「要配慮個人情報」という概念が設けられた。そこでは、本人の「犯罪の経歴」、および「犯罪により害を被った事実」が規定されている。要配慮個人情報については、同意取得が原則化され、第三者提供についてオプトアウト手続によることができないとされている。今後、犯罪の未然防止・再犯防止策における情報の取り扱いの枠組みにおいて、この点の調整が必要となる場面も予想される。これらについては、今後の課題としたい。

人情報を含めた情報を、現行法の枠内で積極的に利用することが、今後、ますます要請されていくことが予想されるように思われる。

そういった要請に迅速、的確かつ合理的に応えていくためには、より網羅的な検討と、そこから、いわば「総論的」な理論を確立していくことが必要となるであろう。本稿は、それにはるかに及ばない内容でしかないことは一目瞭然であるが、それらに向けた今後の検討課題のための一里塚とすることとしたい。今後のさらなる検討に向けて、ひとまずは筆擱くこととする。

本稿は、科学研究費助成事業（基盤研究（C））「技術の高度化等に伴う街頭防犯カメラの新たな利用と法的規制のあり方の検討」（研究課題番号：26380095）による研究成果の一部である。